В.В. Молоков,

кандидат технических наук, доцент
Сибирский юридический институт
ФСКН России (г. Красноярск)

СРЕДСТВА ПРОТИВОДЕЙСТВИЯ РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Незаконный оборот наркотиков с использованием сети Интернет уже довольно давно представляет угрозу обществу и поражает прогрессивную часть молодого поколения.[1] Это связано не только с популярностью интернет-пространства и виртуализацией общения, но и характерной особенностью таких преступлений. В основном это распространение синтетических наркотических средств и психотропных веществ, так называемых спайсов, популярных среди молодежи. Преступная схема такого бизнеса чаще всего основана на бесконтактном способе сбыта, в которой распространитель связан с потребителем исключительно посредством телекоммуникационных каналов сети Интернет. И это с точки зрения явной криминальности такой торговли заставляет организаторов и участников преступных групп скрывать свое присутствие в сети Интернет, усложняя процесс выявления и раскрытия преступлений правоохранительными органами.

Как правило, с незаконным оборотом наркотиков тесно сотрудничают и другие сферы бизнеса, которые обеспечивают техническую, юридическую, информационную поддержку криминального сообщества. Рассмотрим основные средства сокрытия пребывания в сети Интернет и методы анонимизации, используемые распространителями наркотиков.

Технология анонимности в сети Интернет является антагонистом изначальным принципам открытости и безопасности Всемирной паутины. Многое заложено в протоколах сети и не противоречит праву на конфиденциальность личной переписки, журнала посещения страниц и т.п. Основные технологии анонимности составляют прокси-серверы, виртуальные частные сети (VPN), SSH-туннелинг, децентрализованные P2P-сети типа Tor или I2P.

Прокси-сервер (от англ. proxy – право пользоваться от чужого имени) – удаленный компьютер, при подключении к которому он становится посредником для выхода абонента в Интернет. Прокси передает все запросы программ абонента в сеть и, получив ответ,

отправляет его обратно инициатору соединения. Прокси-сервер имеет свой IP-адрес, который открыт со стороны Интернета, но скрывает истинный IP-адрес пользователя. Как правило, прокси-сервер располагается в другой стране, и анализ статистики сайтов, которые посещает абонент, обычно обнаруживает только IP-адрес самого прокси.

VPN (Virtual Private Network – виртуальная частная сеть). Внешне VPN-соединение мало чем отличается от подключения к обычной локальной сети, поэтому приложения без каких-либо настроек используют его для доступа в Интернет. Когда одно из них захочет обратиться к удаленному ресурсу, на компьютере будет создан специальный GRE-пакет, который в зашифрованном виде будет отправлен VPN-серверу. VPN-сервер этот пакет расшифрует, разберется в его назначении и выполнит от своего лица соответствующее действие. Далее, получив ответ от удаленного ресурса, VPN-сервер его снова зашифрует и в таком виде отправит обратно клиенту. Непрерывное шифрование передаваемых данных – это ключевой момент в обеспечении безопасности данного соединения.

SSH (Secure Shell) – сетевой протокол, позволяющий производить удаленное управление компьютером и передачу файлов. Использует алгоритмы шифрования передаваемой информации. SSH-туннелинг можно рассматривать в качестве дешевой замены VPN. Принцип данной реализации следующий: весь сетевой софт на компьютере форвардится (перенаправляется) на назначенный порт (вашего локального хоста), где запущен сервис, соединенный по SSH с удаленным сервером (соединение шифруется) и туннелирующий все запросы. Далее весь трафик абонента (уже в незашифрованном виде) может передаваться с сервера на прокси, который направляет весь поток данных к необходимым адресам.

Tor – это сеть виртуальных туннелей. Типичный представитель децентрализованных сетей, не имеющих центрального узла контроля. Вместо того чтобы идти по прямому пути от отправителя к получателю, пакеты данных в сети Tor выбирают случайные маршруты через несколько серверов, которые скрывают IP-адрес абонента так, что ни один наблюдатель в любой точке не может сказать, откуда или куда направляются данные. Кроме того, в сети информация передается в зашифрованном виде. Инсталлятор пакета Tor ставится без особых сложностей, программа имеет русский интерфейс и представляется в виде преконфигурированного браузера Firefox. Сеть Tor абсолютно бесплатна и ее функциональности обычно хватает для обеспечения анонимности в большинстве слу-

чаев. Фактически отследить абонента через Tor очень тяжело даже для спецслужб, нужно раскручивать гигантские цепочки пользователей и иметь доступ к промежуточным маршрутизаторам.

Существуют и другие сервисы, предоставляющие услуги анонимизации абонента. Обычно организаторы незаконного бизнеса используют приведенные технологии в качестве транспортных сред для работы с коммуникационными программами. Рассмотрим наиболее популярные средства мгновенного обмена сообщениями в сети Интернет (мессенджеры), используемые распространителями наркотиков.

ICQ – централизованная служба мгновенного обмена сообщениями сети Интернет. Пользователь службы работает с программой-клиентом, запущенной на устройстве, соединенном с сетью Интернет. Мессенджер подключается к серверу. Через сервер осуществляется поиск и связь с другими клиентами, а обмен служебными данными и сообщениями между пользователями может осуществляться как через сервер, так и без его участия напрямую. Как и в большинстве мощных сетевых систем, обслуживающих огромное количество клиентских запросов, этот сервер не единственный, и некоторые из них являются кластерами серверов. Следует отметить, что протокол ICQ не является шифрованным и может быть прочитан на канале связи. Вследствие этого злоумышленники не используют его как базовый сервис, а применяют дополнительные средства защиты, которые будут рассмотрены далее.

Jabber – это бесплатный сервис для обмена сообщениями через Интернет на основе открытого протокола XMPP. Для отправки и получения сообщений в Jabber используются серверы, рассредоточенные по всему миру. Одним из таких является сервер проекта Jabnet. Jabber – единственная в мире сеть, сочетающая в себе такие преимущества, как открытость, некоммерческую основу, возможность расширения и множество других полезных особенностей. Одной из таких является служба транспортов, позволяющая без установки дополнительных программ общаться с собеседниками из других сетей (ICQ, QIP, AIM, WLM, Yahoo, Skype и т.п.) так же легко, как и с обычными своими контактами. Вследствие открытости приложения Jabber-сервер можно установить на удаленном хосте за границей и пользоваться личным сервисом сообщений, который, в свою очередь, легко взаимодействует с другими интернет-мессенджерами, тем самым сознательно скрывая местоположение и доступ к хосту.

Telegram – бесплатный мессенджер для смартфонов, позволяющий обмениваться текстовыми сообщениями и медиафайлами различных форматов. Сервис ориентирован на международный рынок и имеет англоязычный интерфейс. Сервис поддерживает сложную систему шифрования переписки. Теоретически все сообщения и хранимые в облаке медиафайлы находятся в полной безопасности.

Brosix – безопасное средство мгновенного обмена сообщениями, которое обладает функциями специально разработанными для промышленных и деловых целей. Приложение Brosix позволяет создавать собственную сеть для мгновенного обмена сообщениями и применяет криптостойкое шифрование. Это делает обмен сообщениями безопасным для передачи конфиденциальной или секретной информации. Подобно Jabber сервис Brosix позволяет установку на удаленных серверах, недоступных правоохранительным органам Российской Федерации.

Skype – бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую и видеосвязь через Интернет (IP-телефония), опционально используя технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны. Передача данных осуществляется в зашифрованном виде, но система дискредитировала себя частыми взломами аккаунтов и разглашением информации о возможности контроля пересылаемых данных правоохранительными структурами. Однако в силу популярности часто используется потребителями наркотиков, которые меньше всего задумываются о безопасности общения.

Таким образом, перечисленные наиболее популярные мессенджеры в той или иной степени позволяют обеспечивать анонимность передаваемой информации, но не всегда защищены от возможности установления IP-адреса абонента сети. В связи с этим сопутствующая индустрия обеспечения информационной безопасности криминального бизнеса постоянно совершенствует технологии сокрытия пребывания в сети и на коммерческой основе предлагает комплексные решения для полной анонимности абонента.

Типовые системы безопасности, как правило, построены по следующему принципу. За границей в одной из лояльных стран арендуется хостинг, на котором разворачивается какой-либо из ранее упомянутых серверов мгновенного обмена сообщениями. Популярным является использование так называемых дедиков (Dedicated Server – выделенный сервер), к которым подключаются законно либо с помощью взлома (хакинга). Соединение с сервером

осуществляется через цепочку анонимных прокси-серверов или VPN-каналов связи. Часто используется транспортный уровень децентрализованной сети Tor, через которую коммутируются все пакеты компьютера абонента. Получается целая цепочка маршрутов прохождения трафика, установить которую в силу изначальной секретности передаваемых данных и отсутствием истории маршрутизации пакетов не представляется возможным. Выделяемые на каналах связи интернет-пакеты содержат IP-адреса серверов, не попадающих под юрисдикцию законодательства Российской Федерации и ее правоохранительных органов.[2] Вопросы международного сотрудничества практически не работают, что не позволяет проводить расследование за пределами сегмента Рунета.

[1] Молоков В.В. Интернет и наркотики // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и нелегального оборота наркотиков : материалы XV международной научно-практической конференции : в 3 ч. Красноярск : СибЮИ ФСКН России, 2012. Ч.1. С. 72-75.

[2] Иванов А.Ю., Ефимов С.Н., Галушин П.В. Противодействие пропаганде наркотических средств и психотропных веществ в сети Интернет // Вестник Сибирского юридического института ФСКН России. 2014. №. 4. С. 37-41.

П.В. Галушин,

кандидат технических наук
Сибирский юридический институт
ФСКН России (г. Красноярск)

ВОЗМОЖНОСТИ АВТОМАТИЗИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ, ПРЕДОСТАВЛЯЕМЫЕ СОЦИАЛЬНЫМИ СЕТЯМИ

Незаконный оборот наркотиков остается одной из острейших проблем, представляющих высокую общественную опасность для личности, общества и государства.

Сервисы сети Интернет, в частности социальные сети, активно используются как для пропаганды наркотических средств и психотропных веществ[1], так и для организации их незаконного оборота[2].

В настоящее время социальные сети развиваются стремительными темпами и охватывают все большее число людей. Так, в одной из самых популярных социальных сетей – Facebook – зарегистрированы более 1,2 миллиарда пользователей, российские социаль-